SALÃO DE INICIAÇÃO CIENTÍFICA XXIX SIC

UFRGS PROPESQ

Salão UFRGS 2017

múltipla UNIVERSIDADE inovadora inspiradora

Evento	Salão UFRGS 2017: SIC - XXIX SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2017
Local	Campus do Vale
Título	Estudo em Teoria de Números: Primalidade em Tempo Polinomial
Autor	WESLEY GONÇALVES LAUTENSCHLAEGER
Orientador	THAÍSA RAUPP TAMUSIUNAS

Título: Estudo em Teoria de Números: Primalidade em Tempo Polinomial

Autor: Wesley Gonçalves Lautenschlaeger

Orientadora: Thaísa Raupp Tamusiunas

Instituição: Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)

Testes de primalidade sempre foram utilizados em diversas áreas da Matemática e da Computação. Entretanto, estes testes possuíam custo exponencial e, consequentemente, eram ineficientes. O teste de primalidade baseado em fatoração, por exemplo, ao testar um primo de aproximadamente 200 casas decimais, levaria mais tempo do que a existência do universo. Em 6 de agosto de 2002 foi publicado o primeiro teste de primalidade que era, ao mesmo tempo, determinístico, incondicional e polinomial: o algoritmo AKS, desenvolvido por Manindra Agrawal, Neeraj Kayal e Nitin Saxena, cientistas da computação do Indian Institute of Technology Kanpur. O algoritmo utiliza Teoria de Grupos e Teoria de Anéis, além de se basear em resultados de outros testes de primalidade, como por exemplo o teste de Fermat. Abaixo será enunciado o algoritmo AKS:

$O\ Algoritmo\ AKS$

$Entrada: inteiro\ n > 1.$

1. $Se\ (n = a^b\ para\ a\ \in\ \mathbb{N}\ e\ b > 1),\ \ escreva\ COMPOSTO.$

2. $Encontre\ o\ menor\ r\ tal\ que\ o_r(n) >\ (\log n)^2.$

3. $Se\ 1 < mdc(a,n) < n\ para\ algum\ a \leq r,\ \ escreva\ \ COMPOSTO.$

4. $Se\ n\ \leq r,\ \ escreva\ PRIMO.$

5. $De\ a = 1\ até\ \left\lfloor \sqrt{\phi(r)}\ \log n \right\rfloor faça$

$se\ \left((X+a)^n\ \not\equiv\ X^n + a\ (mod\ X^r - 1, n)\right),\ \ escreva\ \ COMPOSTO.$

6. $Escreva\ PRIMO.$

Os objetivos do projeto foram desenvolver propriedade matemática, estudar conceitos de Álgebra e de Teoria dos Números e entender a complexidade do algoritmo AKS. Ao decorrer da pesquisa, foram alcançadas otimizações no custo do algoritmo. Nestas otimizações, foram utilizados recursos como o Método de Newton e a convolução realizada no domínio de Fourier, além de resultados da Álgebra Linear e da Teoria dos Crivos.

Com as melhorias aplicadas, o custo do algoritmo sofreu redução do custo original de $[ln\ (n)]^{12}$, onde n se refere ao número inteiro que deseja ser testado, para $[ln\ (n)]^{8}$. A versão com custo mais eficiente já publicada é do matemático estadunidense Carl Pomerance, na qual o custo é $[ln\ (n)]^{6}$. O futuro da pesquisa será baseado na conjectura de Agrawal-Popovych, na qual reduziria o custo do algoritmo original para $[ln\ (n)]^{3}$e, utilizando os métodos de otimização aplicados no projeto, se atingiria um custo ainda mais baixo. Observa-se que o algoritmo de Pomerance não sofreria melhorias com a conjectura, uma vez que foi alterado o passo 5 do algoritmo AKS a qual ela se refere.